UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/739,757	12/20/2000	Seigo Kotani	1466.1023	5419

21171 7590 06/08/2004

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
ADAMS, JONATHAN R	

ART UNIT	PAPER NUMBER
2134	4

DATE MAILED: 06/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/739,757	Applicant(s) KOTANI ET AL.	
	Examiner Jonathan R Adams	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 December 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claim 11 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As to claim 11:

3. Claim 11 states contradictory actions where it states in line 4: "if the target folder if for encipher files..." the file is both enciphered and stored without process. These are contradictory actions.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1, 4, 9, 14, and 15 rejected under 35 U.S.C. 102(b) as being anticipated by Bruce Schneier, "Applied Cryptography".

3. As to claims 1 and 15:

Schneier teaches an encryption method for transmitting and accessing data files using link-by-link encryption with multiple symmetric keys:

Individual key different from communication key used for enciphering / Ek1 (Page 217, Fig 10.1, Schneier)

Individual key used for deciphering / Dk1 (Page 217, Fig 10.1, Schneier)

Communication key for enciphering for transmission / Ek2 (Page 217, Fig 10.1, Schneier)

4. As to claim 4:

Authentication is performed independently for the individual key and the communication key / any to endpoints of the lone need a common key and can change their key independently fro the rest of the network (Page 217, Line, 19, Schneier), Key agreement algorithms can provide authentication (Page 217, Table 10.1, Schneier)

5. As to claims 9 and 14:

Two different keys are authenticated / any to endpoints of the lone need a common key and can change their key independently fro the rest of the network (Page 217, Line, 19, Schneier), Key agreement algorithms can provide authentication (Page 217, Table 10.1, Schneier)

Decoding process using one of the keys / Dk1 (Page 217, Fig 10.1, Schneier)

Enciphering process using the other of the keys / Ek2 (Page 217, Fig 10.1, Schneier)

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 2 and 6-8 rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Barrett et al., US Patent No 5222137 (hereafter referred to as '137).

As to claim 2:

8. Schneier teaches an encryption method for transmitting data using link-by-link encryption across several nodes. Schneier does not teach using different possible keys for each node-to-node connection where an identifier to the key used is added to the data to be transmitted. '137 teaches an encrypted communications system using multiple keys where an identifier to the key used is added to the data to be transmitted (Col 1, Line 58 et seq., '137). It would have been obvious to a person of ordinary skill in the art at the time of invention to use the multiple possible key encryption system with the attached key identifier of '137 with the link-to-link encryption communication system taught by Schneier. One of ordinary skill in the art would have been motivated to use the multiple possible key encryption system with the attached key identifier of '137 with the link-to-link encryption communication system taught by Schneier because providing multiple possible keys reduces the chances that an exterior entity will be able to decipher a key, providing a high standard of security.

9. Schneier further does not teach for the original data file to embed a file identifier into the file name field in the file header. The examiner takes official notice as to embed a file identifier into the file name field in the file header. It would have been obvious to a person of ordinary skill in the art at the time of invention to embed a file identifier into the file name field in the file header. One of ordinary skill in the art would have been motivated to embed a file identifier into the file name field in the file header because it is very well known in the art to use a file name identifier for all files stored on a computer, it is the custom that this identifier be stored in the file name field of the file header.

As to claims 6-8:

10. Schneier teaches an encryption method for transmitting data using link-by-link encryption across several nodes comprising:

- Communication key is used for enciphering data on the transmission side / Ek2 (Page 217, Fig 10.1, Schneier)
- Communication key is used for decoding received data on the reception side / Dk2 (Page 217, Fig 10.1, Schneier)

Schneier does not teach using/preparing different possible keys on the transmission/reception side of each node-to-node connection where an identifier to the key used is added to the data to be transmitted and used during the decoding process. '137 teaches an encrypted communications system using/preparing multiple possible keys on the transmission/reception side of each node-to-node connection where an identifier to the key used is added to the data to be transmitted (Col 1, Line 58 et seq.,

'137) and used during the decoding process. It would have been obvious to a person of ordinary skill in the art at the time of invention to use the multiple possible key encryption system with the attached key identifier of '137 with the link-to-link encryption communication system taught by Schneier. One of ordinary skill in the art would have been motivated to use the multiple possible key encryption system with the attached key identifier of '137 with the link-to-link encryption communication system taught by Schneier because providing multiple possible keys reduces the chances that an exterior entity will be able to decipher a key, providing a high standard of security.

11. Claims 3 and 5 rejected under 35 U.S.C. 103(a) as being unpatentable over Bruce Schneier, "Applied Cryptography".

As to claim 3:

12. Schneier teaches an encryption method for transmitting data using link-by-link encryption across several nodes where data is temporarily stored comprising:

- Communication key used for decoding on reception side / Dk2 (Page 217, Fig 10.1, Schneier)
- Decoded data are enciphered using an individual key different from common key / Ek1, (Page 217, Fig 10.1, Schneier)

13. Schneier further teaches the disadvantage of link-by-link encryption that a data is exposed in intermediate nodes (Page 218, Table 10.2, Schneier). In the link-by-link section Schneier does not specifically teach that a node should delete the exposed plaintext file. In another section Schneier teaches a good cryptography practice to

destroy sensitive plaintext documents stored on a computer (Page 229, Line 16, Schneier). It would have been obvious to a person of ordinary skill in the art at the time of invention to securely delete the plaintext document from intermediate nodes. One of ordinary skill in the art would have been motivated to securely delete the plaintext document from intermediate nodes because Schneier teaches the exposed data as a disadvantage of link-by-link encryption, and later teaches data destruction for aiding in the reconciliation of such a possible security hole.

14. As to claim 5:

Authentication is performed independently for the individual key and the communication key / any to endpoints of the lone need a common key and can change their key independently fro the rest of the network (Page 217, Line, 19, Schneier), Key agreement algorithms can provide authentication (Page 217, Table 10.1, Schneier)

15. Claims 10 and 11 rejected under 35 U.S.C. 103(a) as being unpatentable over Bruce Schneier, "Applied Cryptography" in view of Colvin, Sr., US Patent No 6041123 (hereafter referred to as '123).

As to claim 10:

16. Schneier teaches an encryption method for transmitting data using link-by-link encryption across several nodes comprising:

- Two different keys are authenticated / any to endpoints of the lone need a common key and can change their key independently fro the rest of the network

(Page 217, Line, 19, Schneier), Key agreement algorithms can provide authentication (Page 217, Table 10.1, Schneier)

- If enciphered, the target file is decoded by using one of the keys / Dk2 (Page 217, Fig 10.1, Schneier)
- The other of the keys is used for enciphering the file / Ek1 (Page 217, Fig 10.1, Schneier)

17. Schneier does not teach for a sender to optionally use their own individual key to transmit to the first node in the link-by-link transmission whereby the first node would decrypt the message if encrypted, then reencrypt the message to be sent. '123 teaches cryptographic data communication system where a node decrypts a received message if encrypted and then reencrypts the message to be sent to the receiver (Col 3, Line 10 et seq., '123). It would have been obvious to a person of ordinary skill in the art at the time of invention to use the decryption/reencryption method of '123 with the link-by-link encryption communication system of Schneier. One of ordinary skill in the art would have been motivated to use the decryption/reencryption method of '123 with the link-by-link encryption communication system of Schneier because a first routing node receiving plaintext and ciphertext would need to convert all incoming traffic to a compatible format for a constant receiving party to properly decrypt all messages in the link-by-link taught by Schneier.

18. As to claim 11:

Two different keys are authenticated / any to endpoints of the lone need a common key and can change their key independently fro the rest of the network (Page 217, Line, 19, Schneier), Key agreement algorithms can provide authentication (Page 217, Table 10.1, Schneier)

An enciphered file is decoded by using one of the keys / Dk2 (Page 217, Fig 10.1, Schneier)

It is decided whether a target folder for storing the file is for encipher files / It is inherent that folders of encrypted data could be transmitted in Schneier as modified above

19. Claims 12 and 13 rejected under 35 U.S.C. 103(a) as being unpatentable over Bruce Schneier, "Applied Cryptography" in view of '123 in further view of "Mapping a Network Drive".

As to claim 12:

20. Schneier as modified above teaches an encryption method for transmitting data using link-by-link encryption across several nodes including decoding or enciphering a file store in the first folder when an instruction is performed to move from first computers folder to second computers folder. Schneier as modified above does not specifically teach to display the first folder and second folder. "Mapping a Network Drive" teaches viewing on a display multiple folders across a network for data communications transfers. It would have been obvious to a person of ordinary skill in the art at the time of invention to use a graphical display to display folders across a network as in "Mapping a Network Drive" in the invention of Schneier as modified above. One of

ordinary skill in the art would have been motivated to use a graphical display to display folders across a network as in "Mapping a Network Drive" in the invention of Schneier as modified above because it is very common for computers to use a graphical interface to do networking tasks such as moving files across networks.

21. As to claim 13:

Claim 13 corresponds to claim 10.

Conclusion

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jonathan R Adams whose telephone number is (703) 305-8894. The examiner can normally be reached on Monday – Friday from 10am to 6pm.

23. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100